Cyware AI

Agentic AI Powering Intel, Triage, Response and Beyond

The Security Operations Challenge

Modern SOCs drown in threat intel chaos. Analysts burn hours parsing reports, correlating indicators, and manually enriching IOCs across fragmented feeds, trapped by intel dependencies instead of hunting threats.

How Cyware AI Delivers Agentic Intelligence Across Every Workflow

Purpose-built AI agents autonomously supercharge threat intel operations, slashing manual effort and accelerating threat response from days to minutes. Agents plan, execute, validate, and adapt tasks across the full threat intelligence lifecycle, from intel collection and triage through detection engineering, attack reconstruction, and incident reporting.

Cyware AI

Most AI tells you what it found. Cyware AI acts on it.

- **Faster Access to Critical Threat Intelligence**
- **Accelerate Threat Investigations**
- **Reconstruct Attack Flows and Predict Adversary Behavior**
- **Automatically Engineer Threat Detections from Intel**

Cyware AI Agentic Ecosystem

Accelerate Threat Intelligence Operationalization with Specialized AI Agents

SOC Analysis	**Threat Intelligence**	**Detection Engineering**	**Attack Flow**
Agent	Agent	Agent	Agent
Guides Investigation & Triage	Automates Collection & Analysis	Writes the YARA/Sigma code instantly.	Maps the attack to MITRE ATT&CK.

Incident Reporting	**Alias Consolidation**	**Contextual Intelligence**	**Tag Grouping**
Agent	Agent	Agent	Agent
Standardizes documentation with zero manual effort.	Keeps scoring, rules, and investigations accurate across all agents.	Turns raw intelligence into analyst-ready	Solves taxonomy paralysis for new and scaling

Powering Cyware Products

- Cyware Intelligence Suite
- Cyware Intel Exchange
- Cyware Respond
- Cyware Orchestrate
- Cyware Respond

AI Capabilities Across the Threat Lifecycle

Cyware has also built AI into Cyware Intel Exchange and Cyware Orchestrate. Available today, these capabilities span intelligence gathering, triage, and response.

Stage 1

Intelligence Gathering

Convert web content and reports into structured, enriched threat intelligence automatically powered by the Threat Intel Crawler, Intelligence Parser, and Threat Data Summarization.

Stage 2

Triage and Investigation

Query, correlate, and act on threat data using plain language commands via the Cyware MCP Server.

Stage 3

Response and Reporting

Build, run, debug, and optimize automated response workflows without coding through the Playbook Builder, Runlog Debugger, AI Action Node, and Custom Code Generator.

Enterprise Governance Built In From Day One

Zero Local Storage

No data ever stored on the analyst's device.

Full Audit Logging

Every agent action logged and auditable.

Tenant Isolation

Multi-model backend isolated per tenant.

BYOK Support

Bring Your Own Key for strict compliance environments.

Step Into the Future of Threat Intelligence Actioning With Cyware AI

Book Your Demo Today!